UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
12/955,825	11/29/2010	Bjorn Markus Jakobsson	PARC-20100361-US-NP	8257

35699 7590 07/26/2017

PVF -- PARC
c/o PARK, VAUGHAN, FLEMING & DOWLER LLP
2820 FIFTH STREET
DAVIS, CA 95618-7759

EXAMINER	
OBEID, MAMON A	

ART UNIT	PAPER NUMBER
3685	

NOTIFICATION DATE	DELIVERY MODE
07/26/2017	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

sy_incoming@parklegal.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte BJORN MARKUS JAKOBSSON,
RICHARD CHOW, and RUNTING SHI

Appeal 2016-002373[1]
Application 12/955,825
Technology Center 3600

Before MURRIEL E. CRAWFORD, MICHAEL W. KIM, and PHILIP J. HOFFMANN, *Administrative Patent Judges*.

CRAWFORD, *Administrative Patent Judge*.

DECISION ON APPEAL

STATEMENT OF THE CASE

This is an appeal from the final rejection of claims 1–24. We have jurisdiction to review the case under 35 U.S.C. §§ 134 and 6.

---

[1] Appellants identify Palo Alto Research Center Incorporated as the real party in interest. Appeal Br. 4.

The invention relates generally to "implicitly authenticating a user to access a controlled resource based on contextual data indicating the user's behavior." Spec. ¶ 2.

Claim 1 is illustrative:

> 1. A computer-implemented method for implicitly authenticating a user to access a controlled resource, the method comprising:
>
> receiving, by a computing device from a client device associated with the owner of the device, a request to access the controlled resource;
>
> performing an initial implicit user authentication operation, without prompting the user to perform an authentication-related action, wherein the initial implicit user authentication operation involves:
>
> determining whether the user making the request is the owner of the device based on a user behavior measure calculated using historical contextual data of the owner's past user events; and
>
> in response to determining that the initial implicit user authentication operation failed to authenticate the user based on the owner's historical contextual data, performing a second implicit user authentication to obtain an authentication decision without prompting the user to perform an authentication-related action, wherein performing the second implicit user authentication involves:
>
> collecting additional data associated with the user from one or more devices associated with the owner, wherein the additional data include contextual data different from the historical contextual data;
>
> updating the user behavior measure to incorporate the collected additional data; and
>
> providing the updated user behavior measure to an access controller of the controlled resource to make the authentication decision based at least on the updated user behavior measure.

Claims 1–24 are rejected under 35 U.S.C. § 101 as reciting ineligible subject matter in the form of an abstract idea.

Claim 17 is rejected under 35 U.S.C. § 101 as being an apparatus without structure in the form of software.

Claims 8, 16, and 24[2] are rejected under 35 U.S.C. § 112, fourth paragraph, as being of improper dependent form for failing to further limit the subject matter of a previous claim.

Claims 1–24 are rejected under 35 U.S.C. § 103(a) as unpatentable over French et al. (US 2002/0157029 A1, pub. Oct. 24, 2002) and Constable (US 2008/0189776 A1, pub. Aug. 7, 2008).

We AFFIRM.

ANALYSIS

Rejection of Claims 1–24 under 35 U.S.C. § 101

Appellants argue method claim 1 not an unpatentable abstract idea, because it is "necessarily rooted in computer technology to overcome a problem specifically arising in the realm of computer security and authentication" and "designed to solve a technological problem in 'conventional industry practice,'" (Appeal Br. 16–18), and "because the claimed invention is not 1) a fundamental economic practice, 2) a method of organizing human activities, 3) an idea, in and of itself, or 4) a mathematical relationship or formula" (Reply Br. 8). *See also* Reply Br. 7–18.

[2] Although the Examiner also analyzes and concludes dependent claim 7 is not in proper dependent form, in the Response to Arguments, claim 7 was never rejected under § 112 in the Final Action, and no new grounds of rejection is approved within the Answer. *See* Answer 20. Therefore, we do not consider claim 7 to have been rejected under § 112.

We are unpersuaded by each of Appellants' arguments, for the following reasons.

An invention is patent-eligible if it claims a "new and useful process, machine, manufacture, or composition of matter." 35 U.S.C. § 101. The Supreme Court, however, has long interpreted § 101 to include implicit exceptions: "[l]aws of nature, natural phenomena, and abstract ideas" are not patentable. *E.g.*, *Alice Corp. Pty. Ltd. v. CLS Bank Int'l*, 134 S.Ct. 2347, 2354 (2014).

In determining whether a claim falls within the excluded category of abstract ideas, we are guided in our analysis by the Supreme Court's two-step framework, described in *Mayo* and *Alice*. *Id.* at 2355 (citing *Mayo Collaborative Servs. v. Prometheus Labs., Inc.*, 132 S. Ct. 1289, 1296–97 (2012)). In accordance with that framework, we first determine whether the claim is "directed to" a patent-ineligible abstract idea. *See Alice*, 134 S. Ct. at 2356 ("On their face, the claims before us are drawn to the concept of intermediated settlement, *i.e.*, the use of a third party to mitigate settlement risk."); *Bilski v. Kappos*, 561 U.S. 593, 611 (2010) ("Claims 1 and 4 in petitioners' application explain the basic concept of hedging, or protecting against risk."); *Diamond v. Diehr*, 450 U.S. 175, 184 (1981) ("Analyzing respondents' claims according to the above statements from our cases, we think that a physical and chemical process for molding precision synthetic rubber products falls within the § 101 categories of possibly patentable subject matter."); *Parker v. Flook*, 437 U.S. 584, 594–595 (1978) ("Respondent's application simply provides a new and presumably better method for calculating alarm limit values."); *Gottschalk v. Benson*, 409 U.S.

63, 64 (1972) ("They claimed a method for converting binary-coded decimal (BCD) numerals into pure binary numerals.").

The patent-ineligible end of the spectrum includes fundamental economic practices, *Alice*, 134 S. Ct. at 2357; *Bilski*, 561 U.S. at 611; mathematical formulas, *Flook*, 437 U.S. at 594–95; and basic tools of scientific and technological work, *Benson*, 409 U.S. at 69. On the patent-eligible side of the spectrum are physical and chemical processes, such as curing rubber, *Diamond*, 450 U.S. at 184 n.7, "tanning, dyeing, making waterproof cloth, vulcanizing India rubber, smelting ores," and a process for manufacturing flour, *Gottschalk*, 409 U.S. at 69.

If the claim is "directed to" a patent-ineligible abstract idea, we then consider the elements of the claim—both individually and as an ordered combination—to assess whether the additional elements transform the nature of the claim into a patent-eligible application of the abstract idea. *Alice*, 134 S.Ct. at 2355. This is a search for an "inventive concept"—an element or combination of elements sufficient to ensure that the claim amounts to "significantly more" than the abstract idea itself. *Id.*

Claim 1 is directed to authenticating a user to access a controlled resource by making a determination based on an owner's past behavior, and, optionally, only if the first determination fails to authenticate the user, making a determination based on other data. If the determination leads to authentication, the method ends. The remainder of the claim, therefore, is not necessarily performed, because it is an optional step. *See Ex parte Schulhauser*, Appeal No. 2013-007847, 2016 WL 6277792, at *3–5 (PTAB Apr. 28, 2016) (precedential).

The claimed "controlled resource" is defined as "any resource on a network." Spec. ¶ 24. A network is not defined in the claim. We rely on the ordinary and customary meaning of network as "an interconnected or interrelated chain, group, or system." MERRIAM-WEBSTER ONLINE DICTIONARY (last retrieved on July 20, 2017 at http://www.merriam-webster.com/dictionary/network), and a resource as "a source of information or expertise." *Id.* (last retrieved on July 20, 2017 at http://www.merriam-webster.com/dictionary/resource). These are consistent with the Specification's multiple references to "social networks," which we construe as an interconnected group of people. *See, for example,* Spec. ¶ 38 ("location information of other users in the social network of the observed user helps").

Claim 1 recites receiving information from a "user device," which "can generally include any node on a network including computational capability, a mechanism for communicating across the network, and a human interaction interface." *Id.* ¶ 24. A human interaction interface could, therefore, be a written letter for communication between members of a social network.

Based on the Specification's descriptions of these claim terms, the method is not "deeply rooted" in any specific computer technology, such as "computer security and authentication." Instead, in the broadest, but reasonable, interpretation of claim 1, the method receives a request for access, and then makes a determination "based on a user behavior measure calculated using historical contextual data of the owner's past user events."

As the method merely recites that a determination is made based on historical data, the determination is one that could have been made entirely

through mental thought. The receiving of the request is merely a data input operation, and is considered insignificant extra-solution activity in the form of data gathering. As to the mental determination, the Federal Circuit has held that if a method can be performed by human thought alone, or by a human using pen and paper, it is merely an abstract idea and is not patent-eligible under § 101. *CyberSource Corp. v. Retail Decisions, Inc.*, 654 F.3d 1366, 1373 (Fed. Cir. 2011) ("[A] method that can be performed by human thought alone is merely an abstract idea and is not patent-eligible under § 101."). Additionally, mental processes, e.g., making a determination based on data, as recited in claim 1, remain unpatentable even when automated to reduce the burden on the user of what once could have been done with pen and paper. *Id.* at 1375 ("That purely mental processes can be unpatentable, even when performed by a computer, was precisely the holding of the Supreme Court in *Gottschalk v. Benson*, [409 U.S. 63 (1972)].").

We, therefore, agree with the Examiner that claim 1 is directed to a process that encompasses "purely mental processes." Final Act. 2. Claim 1 is, therefore, directed to an abstract idea.

Turning to the second step of the *Alice* analysis, because we find that claim 1 is directed to an abstract idea, the claim must include an "inventive concept" in order to be patent-eligible, i.e., there must be an element or combination of elements that is sufficient to ensure that the claim in practice amounts to significantly more than the abstract idea itself.

Claim 1 requires a "computing device" only to receive a request, which may simply be a written request, received, for example, in an e-mail. Receiving an e-mail is something a generic computer is capable of performing, which does not satisfy the inventive concept. "[A]fter *Alice*,

there can remain no doubt: recitation of generic computer limitations does not make an otherwise ineligible claim patent-eligible. The bare fact that a computer exists in the physical rather than purely conceptual realm "is beside the point." *DDR Holdings, LLC v. Hotels.com, L.P.*, 773 F.3d 1245, 1256 (Fed. Cir. 2014) (internal citations and quotation marks omitted).

Because claim 1 is directed to an abstract idea, and nothing in the claims adds an inventive concept, the claim is not patent-eligible under § 101. Therefore, we sustain the Examiner's rejection of claim 1 under 35 U.S.C. § 101. We also sustain the rejection of dependent claims 2–8, which further limit the functions that can be performed mentally, and the nature of data upon which those determinations are made. We find no meaningful distinction between independent method claim 1 and either independent medium claim 9, or independent system claim 17; the claims all are directed to the same underlying invention. We, therefore, sustain the rejection of claims 9 and 17, as well as dependent claims 10–16 and 18–24, which recite limitations that do not alter the outcome of the analysis.

Additional Rejection of Claims 17–24 under 35 U.S.C. § 101

We are not persuaded by Appellants' argument that the system recited in claim 17 is eligible subject matter, because "the structure of the system includes interconnected mechanisms" (Appeal Br. 19), and that "the system's interconnected mechanisms provide sufficient structure such that the system is statutory subject matter" (Reply Br. 18).

Claim 17 recites a system with the components of a "user access request receiver," and four mechanism components: a contextual data collecting mechanism, an implicit user authentication mechanism, an

updating mechanism, and an authentication information provision mechanism. The Specification describes an apparatus, which "includes a processor 510, a memory 520, a request-receiving mechanism 540, a user-behavior-modeling mechanism 560, an implicit-authenticating mechanism 530, a behavior measure-adjusting mechanism 550, a data-collecting mechanism 570, and storage 555." Spec. ¶ 52. Claim 17, however, does not recite a processor, memory, or storage.

The Specification describes that "data-collecting mechanism 570 can be any device with a communication mechanism" (*Id.* ¶ 57), the "communication mechanism includes a mechanism for communicating through a cable network, a wireless network, a radio network, a digital media network, etc." (*Id.* ¶ 55), and "implicit authenticating mechanism 530 can be any computing component with a processing logic" (*Id.* ¶ 53). The updating mechanism, and an authentication information provision mechanism are not described.

Two of the four mechanisms are, thus, not described, one is described by reference to a communication mechanism that is circularly defined as a mechanism for communicating, and one is described as having "processing logic." Because claim 17 does not recite the processor, memory, and storage described as being part of the described apparatus, and because the mechanisms are described as performing functions and containing logic, we construe all the mechanisms, and the request receiver, in claim 17 as software modules, configured to perform specific functions.

Claim 17, therefore, recites only software *per se*, which, as the Examiner found, is unpatentable subject matter, because software logic represents pure abstraction. *See* MPEP § 2106 (*citing Gottschalk v. Benson*,

409 U.S. 63, 72 (1972)); *see also* above analysis regarding independent claim 1.

For this reason, we sustain the rejection of claim 17 under 35 U.S.C. § 101 for claiming unpatentable software *per se*. Because claims 18–24, which depend from claim 17, and which were also rejected under 35 U.S.C. § 101, do not alter the analysis, but merely further limit the functions configured into the software "mechanisms," we also sustain the rejection of claims 18–24 as reciting software *per se*.

Rejection of claims 8, 16, and 24 under 35 U.S.C. § 112

Dependent claims 8, 16, and 24 recite "responsive to the updated user behavior measure not meeting the threshold value, prompting the user to perform an authentication-related action."

The Examiner rejects the claim as an improper dependent claim because claim 8 "does not include the limitation 'without prompting the user to perform an authentication-related action' recite[d] by base claim 1," on the basis that it instead does prompt the user. Final Act. 4. Appellants argue claim 8 inherits, and, thus, performs, each step recited in claim 1, and further recites a subsequent step that is "an additional operation performed" after the steps in claim 1 are performed. Appeal Br. 20.

We agree with Appellants, because the additional step in claim 8 prompts the user to perform an authentication, but this does not eliminate the steps performed from claim 1, which are done without prompting a user. For this reason, we do not sustain the rejection of claims 8, 16, and 24 under 35 U.S.C. § 112.

Rejection of Claims 1–24 under 35 U.S.C. § 103(a)

Appellants argue independent claims 1, 9, and 17 together as a group. Appeal Br. 26. We select claim 1 as representative. *See* 37 C.F.R. § 41.37(c)(1)(iv).

We are not persuaded by Appellants' argument that Constable fails to disclose an implicit authentication performed without prompting a user, because Constable discloses embodiments that rely on prompting a user for authentication, such as providing a fingerprint, voice sample, or display of an identification card for a camera. Appeal Br. 27–29. Appellants' arguments are based on embodiments not relied upon by the Examiner, who instead relies on the Constable embodiment of authentication based on location data, provided by a device without prompting a user for that data. Final Act. 6 (citing Constable ¶¶ 7 and 31).

Appellants next argue that Constable does not disclose making a determination about a user "based on a user behavior measure calculated using historical contextual data of the owner's past user events," because, instead, Constable uses information about a user's identity information or about the user's device. Appeal Br. 27–34; *see also* Reply Br. 23 ("The Constable system can only obtain device information and current user location, and does not disclose any techniques or mechanisms for obtaining historical contextual data of the owner's past user events to calculate a user behavior measure without prompting the user."), and 24–26.

The Specification describes that user behavior may be based on location. First, the Specification describes determining user behavior from collected data, in that "[b]ehavioral measure grader 250 receives forwarded user access request 210, contextual data 235 from contextual data collector

230, and a user behavior model 245 from user behavior modeler 240." Spec. ¶ 44. Subsequently, data upon which the user behavior is based originates in contextual data from data collector 230, which "collects contextual data about user 160, and can be any device with a storage and a communication mechanism. Contextual data 235 and contextual data 238 indicate a user's behavior or environment. Examples of contextual data 235 and 238 include locations." *Id.* ¶ 45. We find that location data may, therefore, represent a user's behavior.

Constable discloses "the system can receive location information for the device and the requester as part of the request" and use that location information for making an authentication determination. Constable ¶ 7. Constable, thus, discloses "determining whether the user making the request is the owner of the device based on a user behavior measure calculated using historical contextual data of the owner's past user events," as claimed, by making the determination based on location, which is consistent with the Specification's description of the operation.

We are unpersuaded by Appellants' argument that the combination of French and Constable fail to disclose, in the optional[3] "second implicit user authentication" step, updating a user behavior measure using additional data collected, as claimed. Appeal Br. 35–36; *see also* Reply Br. 31–34.

French discloses a second user authentication step, at "second level authentication process **40**," which "accesses available second type information from data sources." French ¶ 142. Although French prompts the user for this information, Constable discloses authentication based on

[3] The second implicit user authentication step operates only if the first implicit user authentication step fails.

"additional data" to "include contextual data different from the historical contextual data," as claimed, in that Constable's system

> receives from the agent **110** information about the device on which the request is being made. This information received from the agent **110** may include fingerprint data of the device or an arithmetic hash of the data on the device. In one exemplary embodiment, the fingerprint data of the device includes one or more of the following: serial numbers, device configuration (including memory installed, central processing unit speed, etc.). [sic] the health of the device (including whether malware or viruses are installed on the device), whether the hard drive is encrypted, and if a BIOS password or PIN are used on the device.

Constable ¶ 29.

We are persuaded that the ordinary artisan would have recognized that Constable's non-prompted device information could be substituted, for French's prompted information in the second authorization step, to have a second, optional authentication step without user involvement, if the first step fails. *See KSR Int'l. Co. v. Teleflex Inc.*, 550 U.S. 398, 418 (2007) (In making the obviousness determination one "can take account of the inferences and creative steps that a person of ordinary skill in the art would employ.")

We are also unpersuaded by Appellants' argument that combining the disclosures of French and Constable would render both unsuitable for their intended purpose of authenticating users, because, according to Appellants, neither reference is "designed to perform implicit authentication without user input or user action." Appeal Br. 37–38. As noted above, Constable bases user authentication on information received without user prompting, such as location information and device information. *See* Constable ¶ 7.

Therefore, the combination does not render either the teachings of either reference unable to authenticate a user.

Appellants introduce new arguments directed to dependent claims 2 and 4–8 in the Reply Brief, at pages 34–43, but in the Appeal Brief did not address any dependent claims separately. *See* Appeal Br. 26, 38. Appellants have, thus, waived argument about the dependent claims, and we do not address new arguments first presented in the Appeal Brief, because they are not the result of the Examiner's response to the Appeal Brief arguments. *See In re Hyatt*, 211 F.3d 1367, 1373 (Fed. Cir. 2000) (noting that an argument not first raised in the brief to the Board is waived on appeal); *Ex parte Nakashima*, 93 USPQ2d 1834, 1837 (BPAI 2010) (explaining that arguments and evidence not timely presented in the principal Brief, will not be considered when filed in a Reply Brief, absent a showing of good cause explaining why the argument could not have been presented in the Principal Brief); *Ex parte Borden*, 93 USPQ2d 1473, 1477 (BPAI 2010) ("[p]roperly interpreted, the Rules do not require the Board to take up a belated argument that has not been addressed by the Examiner, absent a showing of good cause."); 37 C.F.R. 41.41(b)(2) ("Any argument raised in the reply brief which was not raised in the appeal brief, or is not responsive to an argument raised in the examiner's answer, including any designated new ground of rejection, will not be considered by the Board for purposes of the present appeal, unless good cause is shown.").

For these reasons, we sustain the rejection of independent claims 1, 9, and 17 under 35 U.S.C. § 103(a). We also sustain the rejection of dependent claims 2–8, 10–16, and 18–24, which, effectively, were not argued separately.

DECISION

We affirm the rejection of claims 1–24 under 35 U.S.C. § 101 as reciting ineligible subject matter in the form of abstract ideas.

We affirm the rejection of claims 17–24 under 35 U.S.C. § 101 as software *per se*.

We reverse the rejection of claims 8, 16, and 24 under 35 U.S.C. § 112, fourth paragraph.

We affirm the rejection of claims 1–24 under 35 U.S.C. § 103(a).

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(iv).

AFFIRMED